



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--|-------------|----------------------|-----------------------------|------------------|
| 09/818,658 | 03/28/2001 | Pascal Paillier | 032326-130 | 2508 |
| 21839 | 7590 | 03/08/2006 | | |
| BUCHANAN INGERSOLL PC (INCLUDING BURNS, DOANE, SWECKER & MATHIS) POST OFFICE BOX 1404 ALEXANDRIA, VA 22313-1404 | | | | |
| | | | EXAMINER POLTORAK, PIOTR | |
| | | | ART UNIT 2134 | PAPER NUMBER |

DATE MAILED: 03/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/818,658

Applicant(s)

PAILLIER, PASCAL

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 December 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

In view of the remarks presented by applicant in the Appeal Brief filed on 12/03/05, PROSECUTION IS HEREBY REOPENED.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

1. The Amendment, and remarks therein, received on 12/03/05 have been entered and carefully considered.
2. In light of new arguments presented by applicant in the Appeal Brief, the 35 U.S.C. § 112 and 103 rejections cited in the last Office Action have been withdrawn.

Art Unit: 2134

3. However, consideration of the pending claims identified additional 35 U.S.C. § 101 and 112 issues and a new search has resulted in newly discovered prior art. New grounds of rejection based on the newly discovered prior art follow below.
4. Claims 1-9 have been examined.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 6-9 are directed to non-statutory subject matter.
6. Claim 6 is directed towards mathematic computations (a program that perform certain operations) and fails to produce any useful, concrete and tangible result (the algorithm produced keys not used in any particular process).
7. Claim 7 and 8 also do not offer any useful, concrete and tangible result.
8. Claims 6-9 are directed towards a system (a portable electronic device) claim. However the body of the claims 6-7 and 9 is directed towards a method. Claims may not be directed towards more than one statutory class of invention under the rules set forth under 35 U.S.C. 101.

Claim Objections

9. Claim 5 recite "selecting two integers a, b as candidates. However, it is not clear how these candidates relate to the rest of the claim language.

10. The examiner suggests exchanging the term "candidates" with "a candidate pair".

Claim Rejections - 35 USC § 112

11. Claims 1-4 and 6-9 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

12. In the preamble of claims 6-9 applicant declares that the claim is a system (a portable electronic device) claim. However the body of the claim suggests that it is a method claim. Dependent claims 7-9 continue to recite limitations directed towards the system. As a result it is not clear towards which statutory class claims 6-9 are directed.

13. The essential steps of generating cryptographic keys from two integers a and b are not present in claim 1 but rather it is presented as an additional step in claim 2. In fact applicant seems to introduce some new integers a and b (an integer number a and an integer number b, claim 2) and the limitations 3 and 4 in claim 2 are essentially the same as steps A and B in claim 1. As a result it is not clear whether there are some additional steps or whether claim 2 is uses the same integers and the same calculation as recited in claim 1.

14. Claim 3 recites that "the integer b is predetermined, and the value $a^{\lambda(b)}$ is calculated in advance". It is not clear, in advance to what the value " $a^{\lambda(b)}$ " is calculated. For purposes of further examination the claim limitation is treated as best understood.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

15. Claims 1-7 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Menezes (Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237)* in view of *Weisstein (Eric W. Weisstei, "CRC Concise Encyclopedia of mathematics", 1998, ISBN: 0849396409)*.
16. As per claim 5 *Menezes* teaches a method for generating RSA cryptographic keys comprising steps of selecting two integers a , b ($\neq e$), and verifying whether a and b are co-prime with one another (*Menezes, 8.1 Algorithm, Key generation for RSA public-key encryption, pg. 286*).
17. *Menezes* does not teach that verifying whether a and b are co-prime with one another using Carmichael's theorem (*the theorem includes: calculating a modular exponentiation $a^{\lambda(b)} \equiv 1 \pmod{b}$, where λ is the Carmichael function and verifying whether this modular exponentiation is equal to 1*).
18. However, the limitation of verifying whether a and b are co-prime using the Carmichael theorem is an obvious variant of the RSA method and it is old and well known in the art as evidenced by *Weisstein (Carmichael's theorem, pg. 193)*.
Barring any unexpected results it would have been obvious to substitute RSA

method of verifying whether a and b are co-prime with one another with the Carmichael method.

19. In the method of generating RSA cryptographic keys *Menezes* requires selection of two integers and that the numbers are co-prime to each other. This clearly suggests reiterating steps of co-prime verification (steps B and C) with another pair of numbers.

20. *Menezes* teaches that the numbers a and b that are co-prime are retained in order to generate at least pair of cryptographic keys (*Menezes, pg. 286*).

21. Claim 1 is substantially equivalent to claim 5; therefore claim 1 is similarly rejected.

22. As per claim 2 *Menezes* teaches that the integers a (e) is drawn at random.

Selection of the integer a proceeds selection of the integer b thus the integer b must be stored in memory.

23. As per claim 3 the calculation of the value $\lambda(b)$ precedes generation of electronic keys.

24. As per claim 4 *Menezes* teaches encrypting and/or decrypting information by means of a public key cryptography protocol, using the cryptographic keys as the encryption and decryption keys (*Menezes, 8.3 Algorithm, RSA public-key encryption, pg. 286*).

25. As per claims 6 –7 and 9 *Menezes* in view of *Weisstein* do not explicitly teach that the method disclosed above is performed by a portable electronic device.

26. Official Notice is taken that it is old and well-known practice to use electronic devices to compute and process data (e.g. see definition of a computer in a dictionary). One of ordinary skill in the art at the time of applicant's invention would have been

motivated to use an electronic device to perform a method disclosed by *Menezes* in view of *Weisstein* in order to take advantage of computer's automated processing capabilities.

27. Also, Official Notice is taken that it is old and well-known practice to use portable electronic devices (*e.g. Wood U.S. Patent No. 5675687*). One of ordinary skill in the art at the time of applicant's invention would have been motivated to extend *Menezes* in view of *Weisstein's* invention implemented on electronic devices to portable electronic devices given the benefit of mobility.

28. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Menezes* (*Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237*) in view of *Weisstein* (*Eric W. Weisstei, "CRC Concise Encyclopedia of mathematics", 1998, ISBN: 0849396409*) and further in view of *Yee et al. (U.S. Patent No. 5781723)*.

29. *Menezes in view of Weisstein* teach a method for generating cryptographic keys as discussed above.

30. *Menezes in view of Weisstein* do not teach a portable electronic device that comprise a chip card with a microprocessor.

31. *Yee et al.* teach a portable electronic device that comprise a chip card with a microprocessor (*col. 6 lines 27 and col. 5 lines 27-34*)

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement *Menezes in view of Weisstein's* invention in a portable electronic device as taught by *Yee et al.* One of ordinary skill in the art would have

Art Unit: 2134

been motivated to perform such a modification in order to add cryptographic security protections in the form of data encryption, decryption, signing, and authentication into chip cards.

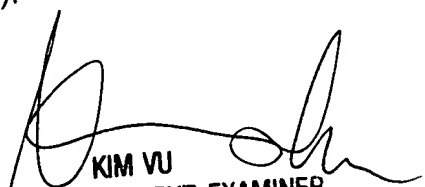
Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


3/1/6


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100